SECURE DATA MANAGEMENT SYSTEM WITH MOBILE DATA MANAGEMENT CAPABILITY

PRIORITY CLAIM TO PROVISIONAL APPLICATION

[0001] This application claims the benefit of the filing date of November 21, 2003 of Provisional Application Serial No. 60/523,685, entitled "Secure Data and Application Mobility Device," under 35 U.S.C. § 119(e).

BACKGROUND OF THE INVENTION

1. Field Of The Invention

[0002] The present invention generally relates to data management, and in particular relates to secure management, backup and recovery of encrypted data from remote and local sites, and access to terminal services resident on remote servers such as corporate servers.

2. Description Of The Background Art

[0003] In a highly mobile society, people want and need continuous access to their electronic data. Whether they are in their homes, their offices or in distant locations while traveling, people need the ability to access their electronic data and applications. Physical security restrictions at airports have made it increasingly burdensome to travel with personal laptop or notebook computers. People also want to protect their data to keep it private. Both individuals and companies have important financial, commercial, legal and personal reasons to maintain their information in a secure and protected state.

[0004] Currently, electronic data is stored on disk drives within portable computers or in various portable memory devices such as flash memory. Typically this data is stored and transported in an unprotected manner. If the portable computers or memory devices are lost or stolen, the data must be considered compromised because even if they are password

protected, these devices can be hacked, passwords uncovered and the data revealed through data recovery programs. Needless to say, data stored in plain text is easily recoverable.

[0005] Additional security problems can occur when using a third party's computer, such as when traveling or when one needs to use a computer immediately but does not have ready access to their own computer. The user has no knowledge of the potential security vulnerabilities of the third party computer, in that there does not exist any easy way to determine if the computer contains viruses or spyware programs that might corrupt or steal their data. Computer security problems in the form of viruses, spyware, and applications that store copies of user data as temporary files without the knowledge of the user are a significant concern. Also, most computer owners rarely keep antivirus and antispyware programs up to date, which makes them vulnerable to infestation by new viruses and spyware.

[0006] The secure mobile transport of data over commercial communication links is a necessity for all government, commercial and individual overseas travelers. The communications of persons on foreign business with their home offices can be an attractive target for eavesdropping and interception by various entities when such persons are in a host country. Because electronic communications usually travel through government-controlled communications media, the threat of interception of such communications from foreign governments is very real.

[0007] Additionally, there presently exists no solution whereby data can be reconstituted in the event of adverse events, such as theft, damage or loss of a portable computer, actions taken by a disgruntled employee to destroy corporate data, system failures or the departure or even death of an employee.

[0008] There are no solutions available today that provide secure data mobility, authentication and access, anti-virus and spyware detection and removal, temporary file identification and removal, automatic unalterable imposition of a corporate security policy, and secure file sharing in a single mobile device that requires no user installation. In addition, it would be desirable for individuals to be able to easily secure and protect their personal data independently of the particular computer or other data processing device they are using.

SUMMARY OF THE INVENTION

[0009] The present invention solves the existing need by providing a secure data management solution that enables secure data mobility, remote and local authentication and access, anti-virus and spyware detection and removal, temporary file identification and removal, and secure file sharing in the form of a portable memory device, such as a single USB device, and that requires no user installation.

[0010] The present invention allows users to securely access data and applications from any data processor system (e.g., a PC, laptop computer, notebook computer, PDA, workstation, remote server, etc.) that is equipped with the appropriate hardware interface and environment with little or no installation process, no configuration of the computer system and no requirement for downloading drivers or other software.

[0011] The user can choose to store data in either secure (e.g., encrypted) or non-secure (e.g., unencrypted) data storage areas. When the user has completed data-related functions, exited programs and removed the memory device there remains no trace of the sensitive data or applications on the computer or other data processing apparatus that was used to access, create or transmit it.

[0012] According to one preferred embodiment, the present invention utilizes a removable memory device, such as a static

memory device with a built-in USB interface, or other removable memory media, in which custom software including applications, configuration information, cryptographic algorithms and user data are contained, and executed by a host computing apparatus when it is coupled to the memory device through the interface.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] The invention will become more clearly understood from the following detailed description in connection with the accompanying drawings, in which:

[0014] FIG. 1 is a diagram of a secure mobile data management system according to a preferred embodiment of the invention;

[0015] FIG. 2 is a diagram illustrating memory device synchronization according to a preferred embodiment of the invention; and

[0016] FIG. 3 is a diagram illustrating memory device access to secure remote software applications according to a preferred embodiment of the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0017] Fig. 1 illustrates one preferred embodiment of a secure mobile data management system according to the present invention, using a management station; however the invention contemplates that the management function could be equally provided by a central server connected to a removable mobile memory device directly through an end-user data processing apparatus. A management station 101 is responsible for issuing a mobile secure memory device 103 to an end user, initializing the device 103 and installing particular applications and data in accordance with the configuration and requirements of the enterprise using the system. The management station 101 communicates with a central server 105

over a communications network 109. The central server is coupled to a database 111.

[0018] The initialization procedure is as follows. At step 1, the memory device 103 is inserted into the management station 101, via an interface such as a USB port, etc. The management station reads the current state of the device 103; if it is a clean device, the management station prepares to configure the device 103 and install appropriate applications for a new user. If the device already contains data or applications, the management station may re-format the device and erase the existing information, may install appropriate applications, or may reject the device and issue an error message.

[0019] At step 2, user identification details are inputted to the management station 101 via a keyboard or other input device to identify the user who is being issued the mobile memory device 103; the management station transmits this information to the central server 105 via the network 109. In this way, all end users are centrally managed and each individual memory device 103 can be individually configured for a unique end user.

[0020] At step 3, the central server retrieves from the database 111 a user profile corresponding to the user identification information sent from the management station. The user profile is used to generate appropriate keys/certificates for the user. If there is no corresponding user profile stored in the database 111 for the end user identification information transmitted from the management station, or if the user profile corresponding to the received identification information already contains an issued key, the central server 105 will identify an error event.

[0021] If the key request is valid, then at step 4 the new key/certificate and memory device issuing details are written to the user profile in the database 111. At step 5, a

response is returned via the network to the management station 101. Where the key issuance request was valid, the central server will send to the management station appropriate key information for storage in the mobile memory device 103. If the request was invalid, then an error message is returned to the management station 101.

[0022] At step 6, the mobile memory device 103 is initialized, its memory is cleared, and software is installed for secure data management and synchronization. Additionally, the user's personal details, configuration settings, and keys/certificates are initially encrypted and then written to the device 103. At step 7, the memory device 103 is physically issued to the user.

[0023] Fig. 2 illustrates an example of operation wherein the memory device is synchronized with the central server. As the user works with data on the mobile memory device 103; the memory device can be synchronized with the central server at periodic or manually-selected intervals to ensure that all data is appropriately backed-up and secure. This synchronization process occurs via a connection over a secure network, or via a secure connection (such as IP Sec, etc.) over an unsecured network, and will securely synchronize all sensitive and encrypted data. At step 1, the user reads current file information from the memory device using a workstation. The user either selects an application option to synchronize files on the memory device, or the device automatically causes the synchronization operation to be performed in accordance with a prestored security policy. This will cause the memory device application to read information on user-selected encrypted and sensitive files from the memory device. The synchronization process also may include polling by the device to retrieve definitional updates for various software applications including, for example, antivirus or antispyware applications.

[0024] At step 2, the user sends read file information to the central server securely over a data network 209. The memory device application will authenticate to the central server repository and send current file information to the central server as a synchronization request. The server also may serve as a conduit for independent secure transfer of files and file collaboration among multiple users.

[0025] At step 3, the server 105 reads the current file state from the database repository 111. The current file state provides to the central server details on the last updated state of the user's files that are stored in the repository. This information is then compared with the user-sent information to determine which files have changed and need to be updated on the central server.

[0026] At step 4, the server 105 sends a file state to the user workstation 107. The file state includes a list of files that need to be sent to the central server in order to fully synchronize the memory device 103 as a response to the initial request. Next, at step 5 the user sends the necessary updated files from the memory device 103 directly to the central server 105, which include all files detailed in the file state response.

[0027] At step 6, the central server writes the updated file to the database repository 111. All new and/or changed files are written to the database. If a file was changed, the old file is retained according to the corporate data retention policies in place. After all files have been correctly synchronized, at step 7 the server 105 returns the details to the user workstation 107. At step 8, the application running on user workstation 107 updates the file information on the mobile memory device 103 to track the last synchronization details.

[0028] FIG. 3 is a diagram illustrating the ability to remotely access sensitive and/or proprietary applications

using the mobile memory device 103. At step 1, the user runs an application access application from mobile memory device 103, by selecting the remote application access function from the memory device 103 and loading the application into the working memory of the user workstation 107; the application executes after reading any necessary keys/certificates from the memory device 103.

[0029] At step 2, the application access application connects to a corporate terminal server 305 by establishing a secured connection with the corporate terminal server through a secure network 209, passing any required keys/certificates to the terminal server 305via the secured connection, and allowing the user to enter any other necessary authentication credentials.

[0030] At step 3, upon completion of a valid authentication, the terminal server 305 establishes a fully connected session with user workstation 107 through the secured network 209 and allows the user to start executing applications as necessary.

Description of Advantageous Features

[0031] The removable memory device application also can provide biometric authentication and access control of the memory device; the secured data management application can provide enterprise access control through an authentication mechanism, and further can provide Local Area Network (LAN) access control through an authentication mechanism.

[0032] The secured data management application provides multilevel authentication, in that each device and system has its own process that it follows to authenticate the user to the system or the device to the system. The first level is the client level and includes the memory device and a host computer. The second level is the management workstation computer. The third level is the repository server.

Additionally, there may be multiple authentication levels within the device or within each of the above levels, such as, for example, biometrics, pass phrases, multiple passwords, etc.

[0033] An integrity check of modular application components is performed to ensure that the memory device uses only approved components, and the removable memory device can provide an application that automatically repairs faulty application components.

[0034] The secured data management application provides encrypted memory device storage of all content to include user data, configuration files, data files, cryptographic algorithms and metadata, and also provides data integrity to ensure that data has not been altered or deleted.

[0035] The removable memory device further contains an application that verifies that all user sensitive data that has been stored as temporary files has been removed from a host computing device, an application that will operate by executing via the removable memory device and will scan and verify that a host computing device is free of user monitoring software. The application will eliminate any spyware or user monitoring software found on a host computing device.

[0036] The security application executes via the removable memory device and scans and verifies that a host computing device is free of virus activity. The application will eliminate any viruses found on a host computing device.

[0037] Multiple pluggable cryptographic algorithms can be maintained on the removable memory device. The user can choose which algorithm she wants to use or the enterprise security policy can determine which algorithm the user must employ for encryption.

[0038] The secured data management application can be integrated into corporate security infrastructures and PKI systems to utilize corporate or commercially issued Keys and

Certificates to encrypt and decrypt user data. The management application issues and revokes user certificates, maintains a Certificate Revocation List (CRL) and cross certifies user certificates with other certificate issuers.

[0039] A management application on the server also can maintain a Centralized User Directory of certificates for the removable memory device user to access and search in the event that they wish to communicate with other users. They can download the certificate, maintain the certificate on their removable memory device and use it to encrypt communications with other users.

[0040] The removable memory device also may maintain a metadata repository pertaining to all files currently stored or registered with the memory device application. The metadata repository can store all unique file identification information, the current file name, file status information, file encryption and algorithm details and other necessary details.

[0041] The removable memory device also may maintain a synchronization request queue of operations to be performed at the next available synchronization process. This process may include operations such as file updates, deletions and other metadata changes.

[0042] The removable memory device can maintain an operating system that is separate from its host computer operating system to ensure that the host computer operating system application cannot change or alter the memory device application. The removable memory device operating system can allow the host computer to boot directly from the removable memory device rather than the internal operating system resident in the computer.

[0043] The removable memory device also may contain an application that hides the file data repository from being viewed to protect it against user manipulation. This

protection is accomplished by tagging the repository directory tree as hidden in the file system. The users never have direct access to files within the repository directory itself, but should be required to access information solely through the removable memory device operating application itself.

[0044] The removable memory device also may provide an encrypted file format to identify and decrypt a file when necessary. The information is bundled with the file in an ASN.1 encoding process.

[0045] The removable memory device also may include an application that provides an automatic file relock for all files that have previously been encrypted. The relock process keeps track of each encryption and decryption event within the application to ensure that all decrypted files are re-encrypted when the user activates the automatic file relock process.

[0046] The removable memory device also may provide data archiving as an alternate to data deletion. The user selects the file, directory or group of files to archive and the data archive process will move the data to a temporary archive location of the device pending the next synchronization process. The synchronization will fully synchronize these archived files to ensure that the server retains the latest versions, and then will mark the server-based copies as archived. Local copies of the files will be deleted.

[0047] The removable memory device can generate a unique file encryption key each time that it is used, such that the loss or disclosure of the file encryption key will not disclose other file keys since each file encryption key is unique to that file.

[0048] The secured data management server may incorporate a web service known as the Simple Object Access Protocol (SOAP) to provide a standardized format for information exchange and to permit change and expansion of that format in the future.

The secured data management server detects shared and concurrent users. The process determines if multiple users are using the same device configuration concurrently with two different memory devices. The purpose of this detection process is to ensure that only the original registered device can be used and other unregistered users can be detected and removed.

[0049] The secured data management server also may provide a group collaboration and sharing channel, which is a channel in which multiple users can read and write files. When a user has permission to join a collaborative channel, they will be given access to a group collaboration and sharing channel. Any file written into this channel will be available to other members after a synchronization process has been completed.

[0050] The secured data management server may also include an application that provides a distribution channel which is a read-only channel. This channel would be intended to provide access to read-only information such as manuals or reference materials.

[0051] The secured data management server may also include an application that provides a process of queuing operations until they can be performed by a connection to the server. The user must be able to queue operations when they do not have a network connection available. If a user chooses to delete a file locally and from the repository, the delete request will be queued and considered for processing when the next synchronization occurs.

[0052] The secured data management server may also include an application that provides a collaboration and sharing directory search process that a user queries to find other users. The search allows for full or partial name matching on users' first names, last names and possible group memberships. The search will return the list of users who match the search parameters.

[0053] The secured data management server may also include an application that provides a secure user-to-user collaboration and sharing process. This process enables a user to send encrypted files to another user. The system provides a directory search menu for the user to search through and to select names to which the user wishes to send files. Once the recipients are chosen, the system retrieves the public keys and IDs for each of the users and encrypts the file headers with a combination of the user's private key and the remote user's public key. This encryption is done within the memory device application to ensure security in transporting the information. These encrypted files are then sent directly to the synchronization server and placed in an incoming queue for the destination user. The file remains queued and will be processed on the next synchronization event.

[0054] The secured data management server may also include an application that provides a secure group collaboration and sharing process that is based on multiple channels and the capability to determine who may subscribe to a channel. The server may be configured to offer multiple channels to a specific company and each channel may have its own access controls placed upon it. A channel can be configured as read only, read-write, or disallowed to read-write. The configuration is determined by the specific user's needs and the security policy limitations for the channel. A channel may not be visible to all users if they are not given read-only access. A default channel can also be denied for specific users. When a channel is subscribed, the user receives all updates placed in the channel, whether the user is read-only or read-write. In the case of conflicting changes by two users, the user will receive an explanation of the problem and a resolution to prevent inadvertent data loss.

[0055] The administration server application uses a relational database to store information about each user of the system. Also stored within the user database is access control and access level information and certificate or key information. The administration server application enables the central corporate server to use the Lightweight Directory Access Protocol (LDAP) as a common source of information about employees in many enterprises.

[0056] The administration server application uses an interface to abstract the User Information Repository (UIR) provider and thus alternate information sources can be used, providing they contain a minimum of information necessary to identify and authenticate users.

[0057] The administration server application ensures that security policy files may be managed on a per-user or a group membership basis. If a user is a member of multiple groups, the server will provide the policy for the first group membership found for the user. If the user is an individual policy file configured user, this policy may take precedence over group policies.

[0058] The administration server application further ensures that a security policy may be configured on a channel-by-channel basis. This configuration would be used most frequently when a channel is to be primarily a read-only channel for most users, but will still allow certain users to upload content and information to it.

[0059] The removable memory device ensures enforcement of server-provided security policies; for example, a policy that would require the removal memory device application to automatically upload new or changed files that are added to the local repository. When the user initiates the synchronization process, the user does not have the option of disabling the uploading portion of the process; or a policy that requires the memory device application to enforce

temporary file removal by the user by eliminating the option of disabling the temporary file cleaning process that can occur when quitting the removable memory device application. The action thus will always occur without user intervention; or a policy that requires pass phrase changes by the user. This setting would allow administrators to set a maximum lifetime for a users pass phrase that is used to protect the removable memory device. At the end of this lifetime the user will be forced to change their pass phrase. This does not impact keys or certificates, but only the pass phrase used to unlock the device.

[0060] The invention having been described, it will be apparent to those skilled in the art that the same may be varied in many ways without departing from the spirit and scope of the invention. Any and all such modifications are intended to be included within the scope of the following claims.